Сравнения по модулю

Определение. Число a делится на натуральное b с остатком r, если $a = bk + r$, причем $0 \leqslant r < b$ и $k \in \mathbb{Z}$. Чтобы найти остаток у числа a при делении на b, нужно из a вычесть ближайшее число, не превосходящее a, делящееся на b.

Например:
Если мы хотим найти остаток для числа $a = 26$ при делении на $b = 4$, то ближайшее не превосходящее a число, которое делится на $b = 4$, равно $24 = 4 \cdot 6$, поэтому $26 = 4 \cdot 6 + 2$ и остаток будет равен $2 = 26 - 24$.

Аналогично это работает и для отрицательных a. Если $a = -5$, $b = 3$, то ближайшее не превосходящее a число, которое делится на 3, равно -6 (не -3, потому что мы ищем не превосходящее число), то есть $-5 = (-3) \cdot 2 + 1$, поэтому у -5 остаток 1 при деление на 3.

Определение. Целые числа, разность которых делится на m, называются сравнимыми по модулю m. Запись: $a \equiv b \pmod{m}$.

Например:
$11 \equiv 6 \pmod 5$, так как 11 - 6 = 5
$2 \equiv 5 \pmod 3$, так как 2 - 5 = -3
$7 \equiv 17 \pmod 5$, так как 7 - 17 = -10
$-4 \equiv 2 \pmod 3$, так как -4 - 2 = -6

Свойства сравнений.

1. $a \equiv b \pmod{m} \Leftrightarrow$ числа a и b дают одинаковые остатки по модулю m.

Замечание. Несмотря на это свойство, если вы хотите проверить сравнимы ли два числа по модулю, то чаще всего удобнее рассматривать их разность, а не пытаться найти остатки для каждого.

2. $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$.

Доказательство. Раз $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, то $a - b$ делится на m и $c - d$ делится на m. Значит их сумма $(a - b) + (c - d) = (a + c) - (b + d)$ тоже делится на m, то есть $a + c \equiv b + d \pmod{m}$

3. $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow a - c \equiv b - d \pmod{m}$.

Доказательство. Аналогично раз $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, то $a - b$ делится на m и $c - d$ делится на m. Значит их разность $(a - b) - (c - d) = (a - c) - (b - d)$ делится на m, то есть $a - c \equiv b - d \pmod{m}$

4. $a \equiv b \pmod{m} \Rightarrow ka \equiv kb \pmod{m}$.

Доказательство. Так как $a \equiv b \pmod{m}$, то $a - b \vdots m$ (выражение $x \vdots y$ означает, что x делится на y), значит $ka - kb = k(a - b) \vdots m$ и $ka \equiv kb \pmod{m}$.

5. $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.

Доказательство. Воспользуемся предыдущем свойством. Так как $a \equiv b \pmod{m}$, то $ac \equiv bc \pmod{m}$ и так как $c \equiv d \pmod{m}$, то $bc \equiv bd \pmod{m}$. Значит у ac и bc одинаковые остатки при делении на m и у bc и bd одинаковые остатки при делении на m, поэтому у ac и bd одинаковые остатки при делении на m и отсюда следует, что $ac \equiv bd \pmod{m}$.

6. $a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m}$ для любого натурального k.

Доказательство. Применяем последнее свойство для $a = c$ и $b = d$ и получим, что $a^2 \equiv b^2 \pmod{m}$. Доказали для $k = 2$. Теперь опять применим последнее свойство для $c = a^2$ и $b = d^2$ и получим, что $a^3 \equiv b^3 \pmod{m}$. Так можно делать сколько угодно раз, поэтому $a^k \equiv b^k \pmod{m}$ для любого натурального k.

Теперь давайте решим пару задач, используя доказанные свойства.

1. Докажите, что число $1000 \cdot 1001 \cdot 1002 \cdot 1003 - 24$ делится
(a) на 999;
(b) на 1004.

Доказательство. Сравнение по модулю позволяют нам заменять числа в выражении на другие, более удобные, числа, которые сравнимы с исходными.

Например, в пунте (a) этой задачи $1000 \equiv 1 \pmod{999}$; $1001 \equiv 2 \pmod{999}$; $1002 \equiv 3 \pmod{999}$; $1003 \equiv 4 \pmod{999}$. Перемножим эти сравнения по 4-ому свойству $1000 \cdot 1001 \cdot 1002 \cdot 1003 \equiv 1 \cdot 2 \cdot 3 \cdot 4 = 24 \pmod{999}$ или $1000 \cdot 1001 \cdot 1002 \cdot 1003 - 24$ делится на 999

В пунте (b) этой задачи $1000 \equiv -4 \pmod{1004}$; $1001 \equiv -3 \pmod{1004}$; $1002 \equiv -2 \pmod{1004}$; $1003 \equiv -1 \pmod{1004}$. Перемножим эти сравнения по 4-ому свойству $1000 \cdot 1001 \cdot 1002 \cdot 1003 \equiv (-4) \cdot (-3) \cdot (-2) \cdot (-1) = 24 \pmod{1004}$ или $1000 \cdot 1001 \cdot 1002 \cdot 1003 - 24$ делится на 1004

2. . Найдите остаток от деления:
(a) 4^{2018} на 3; (b) 6^{2017} на 7; (c) 13^{555} на 9.

Доказательство. (a) $4 \equiv 1 \pmod 3$. По последнему свойству можно возводить в степень, поэтому $4^{2018} \equiv 1 \pmod 3$

(b) $6 \equiv -1 \pmod 7$. По последнему свойству можно возводить в степень, поэтому $6^{2017} \equiv (-1)^{2017} = -1 \pmod 7$. Но –1 — это не остаток, так как оно меньше 0, но -1 дает остаток 6 при делении на 7 (так как $-1 = 7 \cdot 1 + 6$), поэтому 6^{2017} тоже дает остаток 6 при делении на 7.

(c) Так же просто, как и в первых двух пунктах тут не выйдет.
Для начала заменим 13 на 4 ($13^{555} \equiv 4^{555} \pmod 9$) и посмотрим какие остатки дают степени 4 при делении на 9.
$4^1 \equiv 4 \pmod 9$
$4^2 \equiv 16 \equiv 7 \pmod 9$
$4^3 \equiv 7 \cdot 4 \equiv 28 \equiv 1 \pmod 9$

Замечание. Здесь не нужно 4 возводить в 3 степень, достаточно предыдущее сравнение умножить на 4.
$4^4 \equiv 1 \cdot 4 \equiv 4 \pmod 9$

Замечание. Дальше остатки зацикливаются, так как какой остаток дает степень зависит только от того, какой остаток дает предыдущая степень (если $4^{k-1} \equiv r \pmod 9$, то $4^k \equiv 4r \pmod 9$). Здесь можно было бы сказать, что остатки степеней 4 при деление на 9 равны 4-7-1-4-7-1-... и понять, что 555 остаток в этом ряду будет равен 1. Теперь мы знаем, что $4^3 \equiv 1 \pmod 9$ и $555 = 3 \cdot 185$, поэтому возведем сравнение в 185 степень и получим $4^{555} \equiv 1 \pmod 9$.

3. Известно, что $a - 2b$ делится на m и $c - 3d$ делится на m. Докажите, что $ac - 6bd$ делится на m.

Доказательство. Перепишем условие в виде сравнений по модулю m.
Дано:
$a \equiv 2b \pmod m$; $c \equiv 3d \pmod m$
Нужно доказать:
$ac \equiv 6bd \pmod m$, но это и есть произведение двух сравнений, которые нам даны.

Полная система вычетов

Рассмотрим множество всех целых чисел .., -2, -1, 0, 1, 2, ... и разделим их на "мешочки" с цифрами 0, 1, ..., $m-1$, где в мешочке с цифрой k будут давать числа сравнимые с k по модулю m (те, у которых остаток при делении на m равен k). Теперь все числа из одного мешочка можно воспринимать одинаково.

Определение. Полная система вычетов (ПСВ) по модулю m — это набор из m-чисел, дающих всевозможные остатки по модулю m. Так как остатков всего m, то все эти числа должны давать разные остатки по модулю m

Определение. Полная система вычетов (ПСВ) по модулю m — это набор из m-чисел, дающих разные остатки по модулю m. В этом случае очевидно, что в таком наборе будут всевозможные остатки по модулю m, поэтому оба определения равносильны.
(На пальцах: мы из каждого мешочка взяли по одному числу и то множество чисел, которое у нас получилось — это и есть ПСВ)

Свойства ПСВ.

1. ПСВ $+ a =$ ПСВ

Доказательство. От противного. Пусть ПСВ $= (x_1, x_2, ..., x_m)$ и $(x_1 + a, x_2 + a, ..., x_m + a)$ не ПСВ. Тогда по второму определению там должны быть два числа $x_i + a$ и $x_j + a$, у которых одинаковые остатки (иначе это была бы ПСВ), но тогда у x_i и x_j одинаковые остатки, а такого не может быть.

2. $a\cdot$ ПСВ $=$ ПСВ, если НОД$(a, m) = 1$. (Дальше будем писать НОД(a, b), как (a, b))

Доказательство. От противного. Пусть ПСВ $= (x_1, x_2, ..., x_m)$ и $(ax_1, ax_2, ..., ax_m)$ не ПСВ. Тогда по второму определению там должны быть два числа ax_i и ax_j, у которых одинаковые остатки (иначе это была бы ПСВ), тогда $ax_i - ax_j = a(x_i - x_j)$ делится на m и так как $(a, m) = 1$, то $x_i - x_j$ делится на m, но x_i и x_j не могут давать одинаковые остатки.

Замечание. Условие a не делится на m не является достаточным, так как в этом случае из того, что $(x_i - x_j)a$ делится на m не следует, что $x_i - x_j$ делится на m, потому что a и m могут иметь общий делитель больший 1.

Приведенная система вычетов

Определение. Приведенная система вычетов (ПрСВ) по модулю m — это набор из чисел, которые можно получить получить, если взять только те числа, которые взаимно простых с модулем m. (то есть берем только те мешочки, которые взаимно просты с m)

Начнем со случая, когда $m = p$ простое. Тогда мешочек, который делится на p, выпадает из ПрСВ.
Хочется понять, что происходит с ПрСВ, если к ней прибавить a.
К сожалению, ПрСВ + a — это почти никогда не ПрСВ, например, если $p = 5$ и к ПрСВ = [1, 2, 3, 4] прибавить 2, то получится [3, 4, 5, 6], то 5 не взаимно просто с 5.

Давайте сформулируем несколько свойств, который нужно знать про набор чисел, чтобы утверждать, что это ПрСВ:
1) Чисел $p - 1$
2) Все числа взаимно просты с p.
3) Числа из набора дают разные остатки или всевозможные взаимно простые остатки.
Очевидно, что если все остатки разные, то они дают всевозможные остатки и наоборот.

Теперь будем проверять ПрСВ ли это с помощью этого набора из свойств. Давайте поймем, что если умножать ПрСВ на a, такое что $(a, m = p) = 1$, то получится ПрСВ.

Первое свойство очевидно будет выполнено, как и второе из-за того, что $(a, m = p) =$ $= 1$. Пусть третье свойство не выполнено. Тогда должны быть два числа ax_i и ax_j, у которых одинаковые остатки, тогда $ax_i - ax_j = a(x_i - x_j)$ делится на m и так как $(a, m) = 1$, то $x_i - x_j$ делится на m, но x_i и x_j не могут давать одинаковые остатки. Поэтому все три свойства выполнены.

Малая теорема Ферма. Для любого простого p и взаимно простого с p числа a верно, что $a^{p-1} \equiv 1 \pmod{p}$

Доказательство. Давайте возьмем две разные ПрСВ по одному модулю p и перемножим в каждой все числа. Так как наборы остатков одинаковые, то получившиеся произведения будут сравнимы по модулю p.

Тогда рассмотрим две такие ПрСВ: [1, 2, ..., $p - 1$] и [a, $2a$, ..., $(p - 1)a$] (То, что написано справа - это $a\cdot$ ПрСВ) и перемножим в каждой все числа.

Получаем, что $1\cdot2\cdot....\cdot(p-1) \equiv a\cdot2a\cdot....\cdot(p-1)a \pmod{p}$ или $(p-1)! \equiv (p-1)!a^{p-1} \pmod{p}$. Теперь перепишем это через разность, то есть $a^{p-1}(p-1)!-(p-1)! = (a^{p-1}-1)(p-1)!$ делится на p. Из-за того, что НОД($(p - 1)!$, p) $= 1$ следует, что $a^{p-1} - 1$ делится на p или $a^{p-1} \equiv 1 \pmod{p}$

Теорема Эйлера

Появляется вопрос: Можно ли то же самое сказать про составное m? Оказывается, что нет, потому что на $(m-1)!$ нельзя будет сократить, ведь m и $(m-1)!$ не взаимно просты. Для того чтобы получить что-то похожее для составного числа m, мы будем перемножать ПрСВ, но теперь нам нужно, во-первых, как-то посчитать количество элементов в этом наборе, а во вторых, опять проверить, что ПрСВ можно умножать на a, взаимно простое с m.

Начнем с первого пункта. Попробуем найти какую-то закономерность.

Для $m = 5$ есть остатки [1, 2, 3, 4]. Для $m = 6$ есть остатки [1, 5]. Для $m = 10$ есть остатки [1, 3, 7, 9]. Сходу чему равно число элементов в ПрСВ непонятно, поэтому давайте введем функцию Эйлера.

Определение. Значение функции Эйлера $\varphi(m)$ равно количеству натуральных чисел, не превосходящих m и взаимно простых с m или, что то же самое, количество чисел в ПрСВ.

Давайте опять сформулируем несколько свойств, которые нужно знать про набор чисел, чтобы утверждать, что это ПрСВ:
1) Чисел $\varphi(m)$
2) Все числа взаимно просты с m.
3) Числа из набора дают разные остатки или всевозможные взаимно простые остатки.
Очевидно, что если все остатки разные, то они дают всевозможные остатки и наоборот.

Теперь будем проверять ПрСВ ли это с помощью этого набора из свойств. Давайте поймем, что если умножать ПрСВ на a, такое что $(a,\, m) = 1$, то получится ПрСВ.

Первые два свойства очевидно будут выполнены из-за того, что $(a,\, m) = 1$. Пусть третье свойство не выполнено. Тогда должны быть два числа ax_i и ax_j, у которых одинаковые остатки, тогда $ax_i - ax_j = a(x_i - x_j)$ делится на m и так как $(a, m) = 1$, то $x_i - x_j$ делится на m, но x_i и x_j не могут давать одинаковые остатки. Поэтому все три свойства выполнены.

Теорема Эйлера. Для любого числа m и взаимно простого с m числа a верно, что $a^{\varphi(m)} \equiv 1 \pmod{m}$

Доказательство. Давайте возьмем две разные ПрСВ по одному модулю m и перемножим в каждой все числа. Так как наборы остатков одинаковые, то получившиеся произведения будут сравнимы по модулю m.

Тогда рассмотрим две такие ПрСВ: $[x_1, x_2, ..., x_{\varphi(m)}]$ (это любая ПрСВ по модулю m) и $[ax_1, ax_2, ..., ax_{\varphi(m)}]$ (То, что написано справа - это $a\cdot$ ПрСВ) и перемножим в каждой все числа. Получаем, что:
$x_1 \cdot x_2 \cdot .... \cdot x_{\varphi(m)} \equiv ax_1 \cdot ax_2 \cdot .... \cdot ax_{\varphi(m)} \pmod m$ или
$x_1x_2...x_{\phi(m)} \equiv x_1x_2...x_{\varphi(m)}a^{\varphi(m)} \pmod m$.
Теперь перепишем это сравнение через разность, то есть
$a^{\varphi(m)}x_1x_2...x_{\varphi(m)} - x_1x_2...x_{\varphi(m)} = (a^{\varphi(m)} - 1)x_1x_2...x_{\varphi(m)}$ делится на m.
Из-за того, что НОД(x_i, m) = 1, то отсюда следует, что $a^{\varphi(m)} - 1$ делится на m или $a^{\varphi(m)} \equiv 1 \pmod m$

Теорема Вильсона. Пусть p — некоторое простое число. Докажите, что

$$(p-1)! \equiv -1 \ \ (mod\ p)$$

Доказательство. Рассмотрим две такие ПрСВ: $[1, 2, ..., p-1]$ и $[a, 2a, ..., (p-1)a]$. Заметим такой интересный факт, что во втором ПрСВ есть ровно одно число, которое дает остаток 1 при делении на p, то есть существует ровно один такой остаток b, что $ab \equiv 1 \pmod m$. Остаток b называют обратным к a.

Давайте подумаем может ли так случиться, что $a = b$, то есть $a^2 \equiv 1 \pmod m$. Если так произошло, то $a^2 - 1 = (a-1)(a+1)$ делится на p. Значит либо $a-1$, либо $a+1$ делится на p, так как p - простое. Тогда либо $a \equiv 1$, либо $a \equiv -1 \equiv p-1 \pmod m$. (Тут важно, что p — простое, так как если p было бы равно 8, то a могло бы быть равно 5)

Теперь все остатки, кроме 1 и $p-1$, разделим на пары (a, b) такие, что $ab \equiv 1 \pmod m$ и $a \neq b$.

$(p-1)! \equiv 1 \cdot (p-1) \cdot (a_1b_1) \cdot .... \equiv p-1 \equiv -1 \pmod m$, так как в каждой паре произведение сравнимо с 1.

Пример: $p = 7$
$1 \cdot 1 \equiv 1$; $2 \cdot 4 \equiv 1$; $3 \cdot 5 \equiv 1$; $6 \cdot 6 \equiv 1$; Поэтому $6! \equiv 1 \cdot 6 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \equiv -1$

Замечание. В задачах применяется не только сама теорема Вильсона, но и факт о том, что у каждого остатка по модулю p есть обратный.

Теперь давайте порешаем несколько задач на теорему Эйлера.

2. Докажите, что к числу 2^{2018} можно приписать слева несколько цифр так, чтобы снова получилась степень двойки.

Решение. Мы хотим дописать какое-то число цифр слева и получить 2^k. Нужно каким-то образом перевести это на язык остатков и сравнений. Пусть в числе 2^{2018}

n цифр. Тогда для того, чтобы у 2^{2018} и у 2^k совпадали последние n цифр, нужно, чтобы у числа $2^k - 2^{2018}$ последние n цифр были нулями или, что то же самое, чтобы $2^k - 2^{2018}$ делилось на 10^n. Таким образом, наша задача превратилась в следующую задачу: Пусть у числа 2^{2018} в десятичной записи n цифр. Докажите, что найдется такое k, что $2^k \equiv 2^{2018} \pmod{10^n}$.

$2^k - 2^{2018} = 2^{2018}(2^{k-2018} - 1) \vdots 2^n 5^n$. Давайте для начала докажем, что выражение слева всегда делится на 2^n.

Поймем, что первое число, в котором 2019 цифр, это 10^{2018}, но $2^{2018} < 10^{2018}$, поэтому $n \leqslant 2018$, что и дает нам то, что 2^{2018} делится на 2^n.

Теперь осталось найти такое k, что $2^{k-2018} - 1 \vdots 5^n$ или $2^{k-2018} \equiv 1 \pmod{5^n}$. Так как НОД$(2,\ 5^n) = 1$, то здесь можно вспомнить, что по теореме Эйлера $2^{\varphi(5^n)} \equiv 1 \pmod{5^n}$. Значит в качестве k можно взять $2018 + \varphi(5^n)$ и тогда $2^{k-2018} \equiv 2^{\varphi(5^n)} \equiv 1 \pmod{p}$

4. Для скольких значений числа i, где $1 \leqslant i \leqslant 1000$, существует число j, $1 \leqslant j \leqslant 1000$, такое, что $2^j - 1$ делится на i?

Решение. Очевидно, что для четных i число $2^j - 1$ точно не делится на i. Поэтому число i точно нечетное, НОД$(i,\ 2) = 1$, а значит можно применить теорему Эйлера.

$2^{\varphi(i)} \equiv 1 \pmod{i}$, значит если $1 \leqslant \varphi(i) \leqslant 1000$, то тогда $j = \varphi(i)$ нам подходит.

Понятно, что $\varphi(i)$ всегда хотя бы 1, так как для любого числа i есть 1, которая не превосходит i и взаимно проста с i и $\varphi(i)$ всегда не больше i, так как по определению $\varphi(i)$ равно количеству натуральных чисел от 1 до i и взаимно простых с i. Поэтому для всех нечетных i существует требуемое в задаче j

5. Докажите, что для любого натурального числа n найдется число с суммой цифр, равной n, делящееся на n.

Решение. Для начала заметим, что к числу с суммой цифр равной n мы можем дописать сколько угодно нулей справа и при этом сумма цифр не изменится. Поэтому если $n = 2^\alpha 5^\beta k$, где НОД$(k,\ 10) = 1$, то чтобы найти нужное число делящееся на n, достаточно найти число делящееся на k.

Вторая идея этого решения заключается в том, чтобы найти МНОГО чисел с суммой цифр 1 и остатком 1 по mod k. Если мы найдем n таких чисел и сложим их, то сумма цифр сложится (мы на это надеемся), и получившееся число будет сравнимо с n по модулю k, а $n \vdots k$.

В качестве одного из таких чисел можно взять $10^{\varphi(k)}$ (по теореме Эйлера $10^{\varphi(k)} \equiv 1 \pmod{k}$) и тут время вспомнить о том, что сравнения можно возводить в степень, то есть $10^{a\cdot\varphi(k)} \equiv 1 \pmod{k}$, поэтому нам подойдет любое число вида $10^{a\cdot\varphi(k)}$. При сложении n таких чисел в столбик из-за того, что единички у этих чисел будет в разных разрядах, получится число с суммой цифр n и делящееся на k. Осталось лишь дописать к этому число много ($\max(\alpha, \beta)$) нулей справа и получить число с суммой цифр n и делящееся на n.

6. . Докажите, что $2^{2^{..^{2^2}}} - 2^{2^{..^2}}$ (в первом слагаемом n двоек, во втором — $n-1$) делится на все числа от 1 до n.

Замечание. Делится на все числа от 1 до n и делится на $n!$ — это совсем не одно и то же. Например, возьмем $n = 6$: число 60 делится на все числа от 1 до 6, но не делится на $6! = 720$

Замечание. Возведение в степень всегда идет сверху вниз, то есть $2^{2^{2^2}} = 2^{2^4} = 2^{16}$

Решение. Будем доказывать по индукции. Давайте сначала проверим для n = 2. Очевидно, что $2^2 - 2$ делится и на 1, и на 2, а дальше мы будем делать следующее: рассматривать выражение, где в обеих степенях на одну двойку больше и в доказательстве предполагать, что для меньшего количества двоек мы уже все доказали.

(Идея индукции заключается в том, что мы доказываем два факта: если для какого-то числа n наше условие верно, то и для $n+1$ оно тоже будет верно (эта часть решения называется "переход") и что наше условие верно для некоторого минимального числа n, в нашем случае для 2 (эта часть решения называется "база"). Зная эти два факта, мы можем сказать, что раз для $n = 2$ это верно, то и для $n + 1 = 3$ (по 1 факту), а раз для 3, то и для 4 и т. д.)

Базу мы уже доказали, осталось доказать переход.

$2^{2^{..^{2^2}}} - 2^{2^{..^2}} = 2^{2^{..^2}}(2^{2^{..^{2^2}} - 2^{..^2}} - 1)$, степень 2 в скобочках (назовем ее t) — это число из предыдущего шага индукции, то есть t делится на числа от 1 до $n-1$ и нам нужно теперь доказать, что $2^{2^{..^2}}(2^t - 1)$ делится на все числа от 1 до n. Возьмем какое-то число k из ряда от 1 до n и представим k, как $2^x m$, где m нечетное. Теперь нам нужно доказать, что $2^{2^{..^2}}$ делилось на 2^x (это очевидно, так как степень $2^{2^{..^2}} > n \geqslant x$) и $2^t - 1$ делилось на m.

Вторая часть верна, так как $\varphi(m) < m$, если $m \neq 1$ (в случае $m = 1$ утверждение о том, что $2^t - 1$ делится на m очевидно), потому что мы в $\varphi(m)$ рассматриваем числа не превосходящие m и взаимно простые и так как $m \neq 1$, то m не взаимно просто с m, а значит $\varphi(m)$ меньше m хотя бы на 1. Значит $\varphi(m) < n$ и t делиться на $\varphi(m)$,

поэтому $2^t - 1$ делилось на m.

КТО

До этого мы работали только по одному модулю. Интересно, что будет происходить, если рассматривать число сразу по нескольким модулям. Например, если мы знаем, что число сравнимо с 2 по модулю 3, то можем ли мы сказать что-то о числе по модулю 7? Оказывается, что нет, это число может давать любой остаток по модулю. Об этом как раз и говорит Китайская теорема об остатках.

Сформулируем ее сначала для двух чисел

Китайская теорема об остатках Пусть есть два взаимно простых модуля a и b (НОД(a, b) = 1) и есть два остатка x и y. Тогда существует такое число N, что
$N \equiv x \pmod{a}$;
$N \equiv y \pmod{b}$.

Доказательство. Давайте рассмотрим b чисел, которые дают остаток x при делении на a.

$$x, a + x, 2a + x, ..., (b - 1)a + x$$

Если мы докажем, что тут все остатки разные по модулю, то среди них точно будет число с остатком y по модулю b, то есть мы хотим доказать, что наш набор чисел - это ПСВ по модулю b (набор из b чисел с разными остатками по модулю b).

Это так, потому что набор x, $a + x$, $2a + x$, ..., $(b - 1)a + x$ можно получить из ПСВ $0, 1, 2, ..., b - 1$, если сначала домножить на a (так можно делать, так как НОД(a, b) = 1), а затем прибавив x к каждому.

Что же делать, если у нас есть еще условие $N \equiv z \pmod{c}$ и НОД(a, c) = НОД(b, c) = 1? Давайте тогда сначала найдем по только что доказанной теореме такое H, что $H \equiv x \pmod{a}$; $H \equiv y \pmod{b}$. Так как НОД(a, c) = НОД(b, c) = 1, то и НОД(ab, c) = 1, поэтому давайте еще раз используем КТО и найдем такое число $N \equiv H \pmod{ab}$ и $N \equiv z \pmod{c}$. Тогда $N - H$ делится и на a, и на b и
$N \equiv H \equiv x \pmod{a}$;
$N \equiv H \equiv y \pmod{b}$,
$N \equiv z \pmod{c}$
то есть мы опять нашли подходящее N. Давайте сформулируем КТО в общем виде.

Китайская теорема об остатках Пусть числа m_1, m_2, . . . , m_n попарно взаимно просты. Тогда для любых целых a_1, a_2, . . . , a_n найдется целое число x такое, что $x \equiv a_i \pmod{m_i}$ для всех i. Более того, x определен однозначно с точностью до прибавления кратного $M = m_1 m_2 ... m_n$.

Доказательство. Давайте каждому числу от 1 до $m_1m_2...m_n$ сопоставим набор из остатков по модулям m_1, m_2, . . . , m_n (α_1, α_2, ..., α_n).

Сколько максимум может существовать различных наборов остатков? Для α_1 у нас m_1 вариантов, для α_2 у нас m_2 вариантов и т. д., то есть всего $m_1m_2...m_n$ остатков.

Могут ли у двух чисел совпадать наборы остатков? Пусть могут и у X и Y наборы остатков одинаковые. Тогда для любого i $X-Y$ делится на m_i, то есть $X-Y$ делится на $m_1m_2...m_n$, так как числа попарно взаимно просты, но X и Y от 1 до $m_1m_2...m_n$. Противоречие, то есть все наборы разные.

Так как наборов у нас всего $m_1m_2...m_n$ и все они разные, то каждый набор остатков встречается и ровно 1 раз.

Теперь давайте решим пару задач на КТО

3. Найдите наименьшее натуральное число, дающее остаток 2 при делении на 3, остаток 3 при делении на 4, остаток 4 при делении на 5, остаток 5 при делении на 6 и остаток 6 при делении на 7.

Решение. Нам дано:
$x \equiv 2 \pmod 3$;
$x \equiv 3 \pmod 4$;
$x \equiv 4 \pmod 5$;
$x \equiv 5 \pmod 6$;
$x \equiv 5 \pmod 7$
Это можно переписать, как
$x \equiv -1 \pmod 3$;
$x \equiv -1 \pmod 4$;
$x \equiv -1 \pmod 5$;
$x \equiv -1 \pmod 6$;
$x \equiv -1 \pmod 7$
Тогда $x+1$ делится на 3, 4, 5, 6, 7 и на их НОК(3, 4, 5, 6, 7) = 420. Тогда минимальное подходящее x равно 419.

4. Диме выдали натуральное число N. Он разделил его на 101 и получил в остатке $m > 0$. Затем Дима разделил N на m и получил в остатке p. Найдите наибольшее значение p, которое могло получиться, а затем — наименьшее N, при котором это значение p достигается.

Решение. Запишем условие так $N = 101 \cdot k + m$ и $N = mt + p$. Мы знаем, что m — это остаток при деление на 101, поэтому $m \leqslant 100$, аналогично $p \leqslant 99$. Теперь нам нужно проверить, а существует ли такое N для $p = 99$ и $m = 100$, что:

$N \equiv 100 \pmod{101}$ и $N \equiv 99 \pmod{100}$

Если бы нам не нужно было бы находить такое минимальное N, то можно было бы сказать, что по КТО такое N существует и на этом закончить. Сделаем трюк из прошлой задачи $N \equiv -1 \pmod{101}$ и $N \equiv -1 \pmod{100}$. Тогда нам подходит $N = 101 \cdot 100 - 1 = 10099$ и по КТО по модулю 10100 такое N единственное, а значит ответ 10099.

Перейдем на следующий листок.

2. Существует ли такое целое n кратное 4, что n + 4 кратно 9, а n + 9 кратно 25?

Решение. Нас спрашивают существует ли такое n, что $n \equiv 0 \pmod 4$; $n \equiv -4 \pmod 9$; $N \equiv -9 \pmod{25}$. По КТО такой x существует, так как 4, 9, 25 попарно взаимно просты.

Замечание. Часто КТО используют, чтобы задать остатки при делении на разные модули для последовательных (разных) чисел, как в предыдущей и следующей задаче.

7. Назовем число хорошим, если оно делится на квадрат натурального числа > 1. При каких N найдется N последовательных хороших чисел? (Пример для $N = 3$: 48, 49, 50).

Ответ. Для любого N

Решение. Давайте возьмем N различных попарно взаимно простых чисел (например, N простых чисел) p_1, p_2, ..., p_N и захотим, чтобы для какого-то x число $x+1$ делилось на p_1^2, $x+2$ делилось на p_2^2, $x+3$ делилось на p_3^2 и т. д. Такие числа существуют, так как по КТО существует такое x, что:

$x \equiv -1 \pmod{p_1^2}$

$x \equiv -2 \pmod{p_2^2}$

...

$x \equiv -N \pmod{p_N^2}$

8. Докажите, что найдутся 1000 последовательных чисел, каждое из которых не является

(a) простым числом или степенью простого числа;

(b) степенью (не ниже второй) натурального числа.

Решение. Чтобы число не было степенью никакого простого числа, то у него должно быть хотя бы 2 простых делителя. Давайте с помощью КТО найдем такое x, что

$x \equiv -1 \pmod{2 \cdot 3}$

$x \equiv -2 \pmod{5 \cdot 7}$

...

$x \equiv -1000 \pmod{p_{1999} \cdot p_{2000}}$

Тогда такой ряд $x+1$, ..., $x+1000$ подойдет.

Во втором пункте, заметим, что если у числа есть простой делитель ровно в первой степени, то оно точно не степень, то есть если число $A \equiv p \pmod{p^2}$, где p — простое, то A делится на p и не делится на p^2 и тогда A - хорошее

Опять же по КТО найдем такое x, что:
$x + 1 \equiv p_1 \pmod{p_1^2}$
$x + 2 \equiv p_2 \pmod{p_2^2}$
...
$x + 1000 \equiv p_{1000} \pmod{p_{1000}^2}$

Тогда ряд $x + 1$, ..., $x + 1000$ подойдет.

11. Докажите, что числа натурального ряда можно переставить местами так, чтобы для всех n сумма n первых чисел делилась на n.

Решение. Давайте для начала рассмотрим ряд

$$2\ 4\ 6\ 8\ 10\ 12\ldots$$

Сумма первых n будет равна $2 \cdot \dfrac{n(n+1)}{2} = n(n+1) \vdots n$, но этот ряд нам не подходит, потому что в этом ряду у числа 1 не будет места. То есть важно помнить, что в нашем ряду должны быть все числа.

Давайте так и будем составлять наш ряд.
Начнем с 1, 3, 2. Теперь хотелось бы поставить дальше 4, чтобы она не потерялась и была в нашем ряду, но на четвертое место она не подходит, поэтому давайте продлим наш ряд так: 1, 3, 2, x, 4, чтобы $x + 6$ делилось на 4 и $x + 10$ делилось на 5. По КТО такое x (например, $x = 10$) существует и их бесконечно много (так как $x + 20$, $x + 40$, ... нам подойдут). Теперь продолжаем наш ряд 1, 3, 2, 10, 4, y, 5. Хотим, чтобы $y + 20$ делится на 6 и $y + 25$ делится на 7 и по КТО таких чисел очень много.

Теперь давайте сформулируем в общем виде. Пусть у нас есть уже ряд x_1, x_2, ..., x_n. Мы хотим добавить на $n + 2$ место минимальное еще неиспользованное число b. Тогда по КТО мы можем найти такое z, что:
$x_1 + x_2 + ... + x_n + z$ делиться на $n + 1$
$x_1 + x_2 + ... + x_n + z + b$ делиться на $n + 2$
Теперь x_1, x_2, ..., x_n, z, b ряд подходит под условие и минимальное неиспользованное число теперь больше, поэтому найдется момент для любого числа, когда мы его добавим в наш ряд.

Показатели

Мы знаем, что $a^{\varphi(m)} \equiv 1 \pmod m$, если $(a,\, m) = 1$. Может ли a в меньшей степени давать остаток 1 при делении на m? На самом деле может, самый простой случай $a = 1$ или чуть посложнее $a = 2$ и $a^3 \equiv 1 \pmod{m = 7}$, хотя $\varphi(m = 7) = 6$, то есть $\varphi(m)$ не всегда минимальная степень. Тогда давайте назовем эту минимальную степень показателем.

Определение 1. Пусть НОД$(a, m) = 1$. *Показателем* числа a по модулю m называется наименьшее натуральное d такое, что $a^d \equiv 1 \pmod m$. *Обозначение* $\operatorname{ord}_m a$ происходит от английского слова *order*.

Свойства

1. Показатель существует.

Доказательство. Это очевидно, потому что хоть какая-то степень, в которой a сравнимо с 1 существует ($a^{\varphi(m)} \equiv 1$), мы ищем среди натуральных чисел, поэтому существует и минимальная степень.

2. Пусть $\operatorname{ord}_m a = d$. Тогда числа $a, a^2, \ldots, a^d$ попарно не сравнимы по модулю m

Доказательство. От противного. Пусть существует x и y $(x > y)$, что $a^x \equiv a^y \pmod m$ и $a^x - a^y = a^y(a^{x-y} - 1)$ делится на m. Так как $(a,\, m) = 1$, то $(a^{x-y} - 1)$ делится m и тогда мы нашли меньшую степень $(x - y < x \leqslant d)$ такую, что $a^{x-y} \equiv 1 \pmod m$.

3. $a^{d_1} \equiv a^{d_2} \pmod m$ тогда и только тогда, когда $d_1 \equiv d_2 \pmod d$;

Доказательство. Рассмотрим остатки степеней a по модулю m. Мы уже знаем, что первые $\operatorname{ord}_m a = d$ остатков различны и d-ый остаток - это 1. Как мы уже доказывали ранее, все остатки идут по циклу, $d + 1$-ый остаток будет снова равен a и это будет второй остаток, который равен a (так как первые d остатков разные), а значит длина нашего цикла равна d и $a^{d_1} \equiv a^{d_2} \pmod m$ тогда и только тогда, когда $d_1 \equiv d_2 \pmod d$

4. d является делителем числа $\varphi(m)$.

Доказательство. Так $a^{\varphi(m)} \equiv 1 \pmod m$ и длина цикла остатков равна d, то $\varphi(m) \vdots d$

Порешаем несколько задач на показатели

5. Сколько делителей от 1 до 200 имеет число $2^{239} - 1$?

Решение. Пусть $2^{239} - 1$ делится на некоторое $200 \geqslant k \geqslant 1$ и $d = \operatorname{ord}_k 2$, тогда $239 \vdots d$, так как $2^{239} \equiv 1 \pmod k$. Значит $d = 1$ или $d = 239$. Аналогично, $\varphi(k) \vdots d$, так как по теореме Эйлера $2^{\varphi(k)} \equiv 1 \pmod k$ (ее можно применять, так как $2^{239} - 1$ точно не делится ни на какое четное число), но отсюда следует, что $239 > k \geqslant \varphi(k) \geqslant d$, а значит $d = 1$ и $2^1 - 1$ делится на k, то есть k может быть равно только 1.

4. Дано нечетное простое число p, а также простые числа q и r. Известно, что $q^r + 1 \vdots p$. Докажите, что либо $p - 1 \vdots 2r$, либо $q^2 - 1 \vdots p$.

Решение. Давайте сразу перепишем все на язык сравнений. Известно, что $q^r \equiv -1 \pmod{p}$. Возведем это неравенство в квадрат. Получим, что $q^{2r} \equiv 1 \pmod{p}$, значит $2r \vdots d = ord_p q$ и так как r простое, то у d есть 4 варианта для значения.
1 случай $d = 2r$ Тогда по последнему свойству $p - 1 = \varphi(p) \vdots d = 2r$
2 случай $d = 1$ Тогда $q - 1 \vdots p$ и $q^2 - 1 = (p - 1)(p + 1) \vdots p$.
3 случай $d = 2$ Тогда $q^2 - 1 \vdots p$
4 случай $d = r$ Если $r = 2$, то получаеся 3 случай, поэтому давайте считать, что $r \neq 2$. Тогда по последнему свойству $p-1 = \varphi(p) \vdots d = r$ и $p-1 \vdots 2$, поэтому $p-1 \vdots 2r$.

7. Дано простое число p. Докажите, что $2^{2^p} - 4$ делится на $2^p - 1$.

Решение. $2^{2^p} - 4 = 4 \cdot (2^{2^p - 2} - 1)$ должно делиться на $2^p - 1$ и очевидно, что на самом деле мы хотим, чтобы $2^{2^p - 2} - 1$ делилось на $2^p - 1$. Если мы хотим доказать, что степень двойки минус один делится на какое-то число, то нам на самом деле нужно доказать, что $2^p - 2 \vdots ord_{2^p - 1} 2$. Чему же равен $ord_{2^p - 1} 2$? Поймем, что $ord_{2^p - 1} 2 = p$, так как во-первых, p подходит, так как $2^p \equiv 1 \pmod{2^p - 1}$, для $x < p$ $2^x - 1 < 2^p - 1$, поэтому $2^x - 1$ не может делиться на $2^p - 1$. Тогда нам нужно доказать, что $2^p - 2 = 2(2^{p-1} - 1) \vdots p$. Если $p = 2$, то это очевидно, если $p \neq 2$, то это верно по теореме Эйлера.

8. Даны натуральные числа $a, n > 1$. Докажите, что для каждого нечетного простого делителя p числа $a^{2^n} + 1$ число $p - 1$ делится на 2^{n+1}.

Решение. $a^{2^n} \equiv -1 \pmod{p}$, поэтому $a^{2^{n+1}} \equiv 1 \pmod{p}$, а значит $2^{n+1} \vdots d = ord_p 2$. Отсюда следует, что $d = 2^x$, где $x \leqslant n + 1$. Если $x = n + 1$, то $p - 1 = \varphi(p) \vdots 2^{n+1}$ и все хорошо. Если же $x \leqslant n$, то $a^{2^n} = (a^{2^x})^{2^{n-x}} \equiv 1 \pmod{p}$. Противоречие.

Квадратичные вычеты

Пусть мы хотим решить сравнение $x^2 \equiv a \pmod p$ или хотя бы понять существуют ли такие x.

Например, если у нас уравнение $x^2 \equiv 2 \pmod 7$, то есть решения $x \equiv \pm 3 \pmod 7$ и понятно, что это единственные решения, так как $x^2 \equiv 2 \equiv 9 \pmod 7$ и $x^2 - 9 = (x-3)(x+3) \vdots 7$. Но если мы рассмотрим уранение $x^2 \equiv 3 \pmod 7$, то у него уже не будет корней (см. табличку)

x	± 1	± 2	± 3
x^2	1	4	2

Определение. Назовем те $a \neq 0$, для которых сравнение $x^2 \equiv a \pmod p$ имеет ненулевое решение, квадратичными вычетами, а те для которых нет решения, квадратичные невычеты.

Рассмотрим ПрСВ по модулю p

Для начала разберемся с $p = 2$. Заметим, что число $a = 1$ является квадратичным вычетом по любому модулю, так как сравнение $x^2 \equiv 1 \pmod p$ всегда имеет решение $x = 1$. Но так как по модулю 2 всего один класс вычетов отличный от 0, это $a \equiv 1 \pmod 2$, то для $p = 2$ любое нечетное число по модулю два является квадратичным вычетом. Далее везде считаем $p > 2$, так как $p = 2$ – не самый интресный случай.
Пусть $p > 2$, рассмотрим ± 1, ± 2, ..., $\pm \dfrac{p-1}{2}$ и возведем их в квадрат. Получим
1, 4, ..., $(\dfrac{p-1}{2})^2$
Могут ли в этом ряду быть 2 числа с одинаковыми остатками по модулю p? Пусть $x^2 - y^2 \vdots p$, то есть либо $x = y$, либо $x + y \vdots p$, но $0 < x, y \leqslant \left(\dfrac{p-1}{2}\right)^2$. Противоречие. Значит они все разные, то есть квадратичных вычетов всегда $\left(\dfrac{p-1}{2}\right)^2$, поэтому квадратичных невычетов тоже $\left(\dfrac{p-1}{2}\right)^2$.

Свойства вычетов

1. Если квадратичный вычет умножить на квадратичный вычет, то получится квадратичный вычет.

Доказательство. Если a — квадратичный вычет ($x^2 \equiv a \pmod p$) и b — квадратичный вычет ($y^2 \equiv b \pmod p$), то ab тоже квадратичный вычет, ведь $(xy)^2 \equiv ab \pmod p$.

2. Если квадратичный вычет умножить на квадратичный невычет, то получится квадратичный невычет.

Доказательство. Если a — квадратичный вычет ($x^2 \equiv a \pmod p$), то если ПрСВ (1, 2, ..., $p-1$) умножить на a, мы получим ПрСВ (a, $2a$, ..., $(p-1)a$). Количество

квадратичных вычетов и квадратичных невычетов осталось тем же и мы знаем, что если квадратичный вычет умножить на a, то получится снова квадратичный вычет, а значит при умножении на a квадратичные невычеты тоже останутся квадратичными невычетами.

3. Если квадратичный невычет умножить на квадратичный невычет, то получится квадратичный вычет.

Доказательство. Проведем аналогичные рассуждения. Если d — квадратичный невычет, то если ПрСВ 1, 2, ..., $p-1$ умножить на d, мы получим ПрСВ d, $2d$, ..., $(p-1)d$. Количество квадратичный вычетов и квадратичный невычетов осталось тем же и равно между собой, мы знаем, что если квадратичный вычет умножить на d, то получится квадратичный невычет, а значит при умножении на d квадратичные невычеты станут квадратичными вычетами.

Рассмотрим сравнение $x^2 \equiv a \pmod p$ и возведем его в степень $\frac{p-1}{2}$.
$1 \equiv x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod p$, то есть (кв. вычет)$^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Теперь давайте поймем с чем сравнимо $T = b^{\frac{p-1}{2}}$, если b невычет. Заметим, что $T^2 = b^{p-1} \equiv 1 \pmod p$, поэтому $T^2 - 1 = (T-1)(T+1) \vdots p$, то есть $b^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$, но у уравнения $x^{\frac{p-1}{2}} \equiv 1$ есть не больше $\frac{p-1}{2}$ корней по модулю p (Доказательство этого факта мы опускаем, так что вам придется в него поверить) и очевидно, что это квадратичные вычеты, поэтому для квадратичного невычета $b^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Определение 2. *Символом Лежандра* называется выражение, обозначаемое $\left(\frac{a}{p}\right)$ (для $p > 2$), которое определяется следующим образом:

- $\left(\frac{a}{p}\right) = 1$, если a — квадратичный вычет по модулю p;
- $\left(\frac{a}{p}\right) = -1$, если a — невычет по модулю p;
- $\left(\frac{a}{p}\right) = 0$, если a кратно p.

Свойства символа Лежандра.

(a) вычетов и невычетов поровну — по $\frac{p-1}{2}$ штук;

(b) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$ (критерий Эйлера);

(c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ (мультипликативность).

Доказательство. Первые два свойства мы доказали выше.
Если a —квадратичный вычет, то $\left(\frac{a}{p}\right) = 1 \equiv a^{(p-1)/2} \pmod p$.

Если b —квадратичный невычет, то $\left(\frac{b}{p}\right) = -1 \equiv b^{(p-1)/2} \pmod{p}$.

$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$

Теперь порешаем задачи на вычеты.

4. Докажите, что -1 является квадратичным вычетом по модулю $p \iff p = 4k+1$.

Решение. -1 является квадратичным вычетом по модулю $p \iff 1 =$
$= \left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p} \iff (-1)^{(p-1)/2} = 1 \iff p = 4k+1$.

5. Докажите, что у сравнения $(x^2-2)(x^2-3)(x^2-6) \equiv 0 \pmod{p}$ всегда есть решение.

Решение. Если $p = 2$ или $p = 3$, то нам подойдет $x = p$. В остальных случаях у сравнения будет решение $(x^2-2)(x^2-3)(x^2-6) \equiv 0 \pmod{p}$ если 2, 3 или 6 будут кв. вычет, то есть единственный случай, который нам не подходит — это $\left(\frac{2}{p}\right) = -1$, $\left(\frac{3}{p}\right) = -1$, $\left(\frac{6}{p}\right) = -1$, но $\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{6}{p}\right)$. Противоречие.

9. Докажите, что простых чисел вида $4k+1$ бесконечно много.

Доказательство. Очевидно, что простых чисел бесконечно много. Все простые делятся на 3 группы:
$p = 2$;
$p = 4k+1$;
$p = 4k+3$.
Докажем для начала, что чисел вида $4k+3$ бесконечно много от противного. Пусть p_1, ..., p_n - все числа вида $4k+3$. Рассмотрим число $4 \cdot p_1 \cdot ... \cdot p_n - 1$. У него нет делителей вида $4k+3$ и оно нечетно, поэтому все его простые делители вида $4k+1$, но само число сравнимо с -1 по модулю 4. Противоречие.

Вернемся к нашей задаче. Мы знаем, что -1 бывает квадратичным вычетом только по простому числу вида $4k+1$, поэтому если $x^2+1 \vdots q$ для нечетного простого q, то $x^2 \equiv -1 \pmod{q}$, $\left(\frac{-1}{q}\right) = 1$ и q — простое число вида $4k+1$. Опять представим, что количество простых чисел вида $4k+1$ конечное число и вот они q_1, ..., q_m. Рассмотрим число $(2q_1...q_m)^2+1$, оно не делится на 2, у него нет делителей вида $4k+3$ (так как если $x^2+1 \vdots q$ для нечетного простого q, то q — простое число вида $4k+1$) и оно не делится ни на одно простое число $4k+1$. Противоречие.

Первообразный корень

Мы говорили, что если $d = ord_m a$, то a, a^2, ..., a^d будут разные остатки, но хотелось бы, чтобы это были не просто различные остатки, но и всевозможные по модулю m.

Например, если $m = 7$, то рассмотрим $a = 3$.
$3 \equiv 3 \pmod 7$
$3^2 \equiv 2 \pmod 7$
$3^3 \equiv 6 \pmod 7$
$3^4 \equiv 4 \pmod 7$
$3^5 \equiv 5 \pmod 7$
$3^6 \equiv 1 \pmod 7$

Определение. Число называется *первообразным корнем (primitive root)* по модулю m, если его показатель равен в точности $\varphi(m)$.

Теорема. По любому простому модулю p существует первообразный корень.
Для начала докажем полезную лемму.
Ключевая лемма. Докажите, что если показатели каких-то двух чисел a и b равны d и k соответственно такие, что $(d,\, k) = 1$, то существует число, показатель которого равен $ord_p ab = dk$.

Доказательство. Во-первых, $(ab)^{dk} \equiv (a^d)^k (b^k)^d \equiv 1 \pmod p$. Осталось понять почему эта степень минимальная. Пусть $ord_p ab = t$. Тогда $(ab)^t \equiv 1 \pmod p$.

Возведем в степень k. $(ab)^{kt} \equiv a^{kt}(b^k)^t \equiv a^{kt} \equiv 1 \pmod p$, то есть $kt \vdots ord_p a = d$ и $t \vdots d$, так как $(d,\, k) = 1$. Аналогично $t \vdots k$, то есть $t \vdots dk$, значит $t = dk$

Теперь вернемся к доказательству теоремы.

Доказательство. Пусть $d_1, \ldots, d_{p-1}$ — показатели чисел $1, \ldots, p-1$ соответственно.

НОК$(d_1, \ldots, d_{p-1}) = q_1^{\alpha_1}, , q_n^{\alpha_n}$. Тогда есть $d_i \vdots q_1^{\alpha_1}$.

Если у a показатель dk, то хочется сказать, что у числа a^d показатель k, ведь $a^{dk} - 1 \vdots p$ и если существует $k_1 < k$ такой, что $a^{dk_1} - 1 \vdots p$, то у a показатель был бы меньше.

Раз $d_i \vdots q_1^{\alpha_1}$, то $d_i = q_1^{\alpha_1} \cdot X$. Значит существует число (i^X), у которого показатель $q_1^{\alpha_1}$. Тогда найдем такие числа для каждого простого q_j и перемножим их. По предыдущей лемме у произведения показатель будет НОК$(d_1, \ldots, d_{p-1})$.

Осталось доказать, что $H = \text{НОК}(d_1, \ldots, d_{p-1}) = p - 1$

$p - 1 \vdots d_i = ord_p i$ по свойству показателя. Значит $p - 1 \vdots H$ и $p - 1 \geqslant H$.

Давайте рассмотрим сравнение $x^H \equiv 1 \pmod{p}$. С одной стороны, корней не больше, чем H. С другой стороны, $H \vdots d_i$ для любого i, поэтому $i^H \equiv 1 \pmod{p}$, то есть решений хотя бы $p - 1$ и $H \geqslant p - 1$. Соединяем 2 последних факта и получаем, что $H = p - 1$, то есть мы найдем первообразный корень.

Минутка анекдотов про цирюльника Приходит католический пастор к цирюльнику.
Постриг тот его, пастор спрашивает:
- Сколько с меня?
- Нисколько, ваше преподобие. Я с католических пасторов денег за стрижку не беру.
Приятно удивленный, пастор удалился. На другой день приходит цирюльник и видит под дверями парикмахерской 12 бутылок лучшего монастырского вина.

Вскоре приходит православный поп к цирюльнику. Постриг цирюльник и его.
Поп спрашивает:
- Сколько я вам должен, голубчик, за стрижку?
- Да нисколько, батюшка. Православных священников стрижем бесплатно.
На следующее утро цирюльник нашел у дверей парикмахерской 12 бутылок водки.

Еще через несколько дней приходит к цирюльнику раввин. Постриг его цирюльник, а раввин и спрашивает:
- Сколько вам заплатить?
- Да нисколько, уважаемый ребе. Раввинов мы стрижем бесплатно.
Раввин, обрадованный таким оборотом дела, ушел.

На следующее утро цирюльник увидел у дверей своей парикмахерской двенадцать... раввинов!!!..

Только что мы доказали, что по любому простому модулю p существует первообразный корень g. Теперь мы можем представить все остатки, как $g, g^2, \ldots, g^{p-1}$.

Подумаем о том, какие из этих степеней являются кв. вычетами.

Очевидно, что g в четных степенях $(g^2, g^4, \ldots, g^{p-1})$ — это и есть все кв. вычеты, так как каждое из них квадрат и g в нечетных степенях — это кв. невычета, так как в обратном случае $g^{2k+1} \equiv x^2 \pmod{p}$; $g^{(2k+1)\cdot(p-1)/2} \equiv g^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$, а такого не может быть, так как все остатки $g, g^2, \ldots, g^{p-1}$ различны и $g^{p-1} \equiv 1 \pmod{p}$.

Теперь давайте подумаем: сколько существует разных первообразных корней по модулю p?

Мы хотим понять, когда g^k — это первообразный корень. Пусть $d = ord_p g^k$

$g^{kd} \equiv 1 \pmod p \leftrightarrow kd \vdots p-1$ То есть если k взаимно просто с $p-1$, то $d = p-1$, а если k не взаимно просто с $p-1$, то $d = \frac{p-1}{(p-1,k)}$

Доказательство теоремы Вильсона
$(p-1)! \equiv gg^2 \dots g^{p-1} \equiv g^{p\frac{p-1}{2}} \equiv g^{(p-1)\frac{p-1}{2}} g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod p$
С одной стороны $g^{\frac{p-1}{2}}$ не сравним с 1, с другой стороны при возведение в квадрат получаем $g^{(p-1)} \equiv 1 \pmod p$, поэтому $(p-1)! \equiv g^{(p-1)/2} \equiv -1 \pmod p$

Пусть $p-1 = kd$. При возведении в степень k ПрСВ $g, g^2, \dots, g^{p-1}$ мы получаем $g^k, g^{2k}, \dots g^{dk} = 1, g^{(d+1)k} = g^k, \dots, g^{(p-1)k}$ и очевидно, что здесь будет ровно d различных остатков. Это бывает полезным в случаях, если в задаче речь идет про 5-ые степени, то удобно говорить про модуль одиннадцать, так как получится всего 2 различных остатков $(g^5, g^{10}, g^{15} = g^5, g^{20} = g^{10}, ...)$

3. Докажите, что натуральные числа 1, 2, ..., 238 можно расставить по кругу так, чтобы для любых трех подряд идущих по часовой стрелке чисел a, b, c число $b^2 - ac$ делилось на 239.

Решение. Будем воспринимать наши числа 1, 2, ..., 238, как $g, g^2, \dots, g^{p-1}$, где g — первообразный корень и будем их расставлять по кругу, так как нас интересует значения чисел лишь по модулю 239. Расставим из по кругу так $g, g^2, \dots, g^{p-1}$. Для чисел g^{i-1}, g^i, g^{i+1} очевидно, что $g^{2i} - g^{i-1}g^{i+1}$ делится на 239, поэтому наша конструкция подходит для всех чисел не на стыке. На стыке все тоже хорошо, так как числа g и g^2 можно представить, как g^p и g^{p+1}.

6. Дано простое число p и натуральное число $0 < i \leqslant p-2$. Докажите, что

$$1^i + 2^i + \ldots + (p-1)^i \vdots p.$$

Решение. Первое, что мы делаем — это заменяем все остатки на степени g. Тогда

$$1^i + 2^i + \ldots + (p-1)^i \equiv g^i + g^{2i} + \ldots + g^{(p-1)i} = g^i \frac{g^{(p-1)i} - 1}{g^i - 1}$$

Числитель делится на p, так как $g^{p-1} \equiv 1 \pmod 1$ и так как $0 < i \leqslant p-2$, то знаменатель не делится на p, поэтому эта сумма делится на p.

Рождественская теорема Ферма Для любого простого числа p вида $4k+1$ можно представить, как сумму двух квадратов.

Решение. Для начала скажем, что для простого числа $p = 4k + 3$ не существует представления в виде $x^2 + y^2$. Это так из-за того что квадраты дают только остатки 0 и 1 по модулю 4, а значит $x^2 + y^2$ может давать только остатки 0, 1 и 2.

Для начала докажем лемму Туэ.

Лемма Туэ. Пусть n — натуральное число, а a — целое. Тогда найдутся такие целые x и y, что $(x, y) \neq (0, 0)$, $ax - y \vdots n$, и $|x|, |y| \leqslant \sqrt{n}$.

Доказательство. Рассмотрим такие пары $(x,\ y)$, что $0 \leqslant x \leqslant \sqrt{n}$, $0 \leqslant y \leqslant \sqrt{n}$ (исключая $(0,\ 0)$). Вариантов для значения x ровно $[\sqrt{n}]+1 > \sqrt{n}$ $(0,\ 1,\ ....,\ [\sqrt{n}])$ и вариантов для y аналогично $> \sqrt{n}$, поэтому пар $> n$ или $\geqslant n+1$, но нам нужно выкинуть $(0,\ 0)$, поэтому пар $\geqslant n$. Для каждой пары можно посчитать значение $ax - y$ и либо у нас найдется такая пара, в которой $ax - y$ делиться на n, либо для всех пар значений $ax - y$ не делится на n. Тогда так как пар хотя бы n, то найдутся 2 пары (x_1, y_1) и (x_2, y_2) такие, что для них $ax_1 - y_1$ и $ax_2 - y_2$ имеет одинаковый остаток по модулю n. Тогда $(ax_1 - y_1) - (ax_2 - y_2) = a(x_1 - x_2) - (y_1 - y_2)$ делиться на n, $\sqrt{n} \geqslant x_1 - x_2 \geqslant -\sqrt{n}$ и $\sqrt{n} \geqslant y_1 - y_2 \geqslant -\sqrt{n}$, то есть мы нашли подходящие $x = x_1 - x_2$ и $y = y_1 - y_2$.

Возвращаемся к доказательству теоремы. Так как $p = 4k + 1$, то -1 — кв. вычет по модулю p, поэтому существует такое a, что $a^2 \equiv -1 \pmod{p}$. Найдем x, y по лемме Туэ для такого a. Имеем $ax \equiv b \pmod{p}$, возведем данное сравнение в квадрат и получим $-x^2 \equiv (ax)^2 \equiv b^2 \pmod{p}$, возьмем $y = b$, получаем $x^2 + y^2 \vdots p$ и $0 < x^2 + y^2 < \sqrt{p}^2 + \sqrt{p}^2 = 2p$, так как $(x, y) \neq (0, 0)$ и $x \neq \sqrt{p}$, потому что p простое и x целое.
$x^2 + y^2$ от 1 до $2p - 1$ и делится на p, поэтому $x^2 + y^2 = p$.